This document contains excerpts from the Expendable Launch Vehicles (ELV) Independent Assessment Report (title page shown below). Only those sections which relate to the PBMA element **Software Design** are displayed.

The complete report is available through the PBMA web site, Program Profile tab.

3.2 Probable Causes and Assurance Process Gap Analysis

ELV Failure Case Studies and Gap Analysis

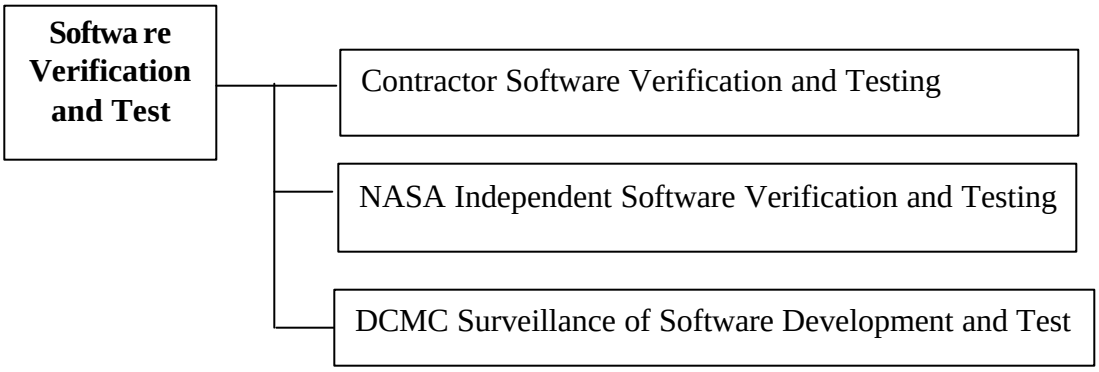
	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
3.	**Delta III: 26 Aug 98-Booster Failure** Human error in assumptions regarding applicability of Delta II software on the Delta III vehicle.	Used Delta II software on a Delta III, i.e. wrong application of software. Delta II control software assumed 4 Hz structural vibration modes would be damped (converging toward zero). Classic "heritage trap".	NASA/ELV mission analysis group looks closely at changes to core vehicle software.	Medium
6.	**Titan IV-B32: 30 Apr 99-Upper Stage Centaur Software Failure (DoD)** Incorrect flight constant was manually entered into the Centaur software. Human error.	Centaur flight software verification failure. Software experts consulted at GRC do not believe that KSC or GRC would have detected the coding error. One lessons learned, identified by GRC in the failure review, is to have the controls team evaluate the frequency response (Bode Plots) of "implemented software" to verify proper performance.	It is not likely that the NASA/ELV mission analysis group working with LMA would have detected this failure mode. The LMA controls group verified the filter constants (through simulation) but the constant was coded improperly (manual entry) by the software group. The FAST simulation does not exercise the Inertial Measurement System (IMS) software where the error occurred.	Low

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
24.	**Conestoga 1620: 23 Oct 95- Unintended Thrust Vector Actuation Signal Was Sent To The Castor IVB Nozzle Actuator** No software filters to reduce noise to the onboard navigation computer.	Fundamental design flaws in hydraulics, software, and vehicle modal analysis. Latent design defects. If first flight or qualification flight NASA MSFC (in support of KSC engineering) may have detected design defects.	NASA design/engineering may or may not have identified failure modes in initial vehicle qualification. Post initial qualification NASA would not have been in a mode to capture a latent design defect.	Medium

A.5 Software Verification and Test Assurance Processes

NASA has approval authority over contractor test methods and data used to verify mission-unique software and some modifications to core vehicle software. NASA exercises insight for routine software verification activities. Software verification testing may be conducted by NASA in cases where complex high-value spacecraft are involved. Formal software design reviews are routinely employed and independent assessment is conducted on a case by case basis.

Historically, the verification of guidance and flight software for NASA ELV missions has been implemented somewhat differently by the responsible design centers (GRC or GSFC), reflecting differences in launch vehicle design and mission needs. For the Atlas/Centaur vehicle, emphasis has been placed on guidance and sequencing through review of software test results. Various guidance accuracy analysis tasks have also been performed. For the Delta II and Pegasus vehicles, the emphasis has been placed on software design reviews and review of relevant mission and core vehicle documents. Specific analysis tasks have also been performed when warranted.



KSC is currently developing an integrated software IV&V approach which will combine aspects of the historical Delta and Atlas approaches. This should allow KSC to understand and review the launch service provider process that they use for software verification and assure that all necessary items have been checked. The capability to perform this insight will be applied, as necessary, for all ELV's under KSC responsibility. Mission-unique changes to core vehicle flight software will be reviewed. It is expected that the basic core vehicle flight software will be well understood and checked out for each NASA mission. This checkout will begin with the start of the mission integration process and continue through final documentation of the flight software. Core software is seldom changed for the more mature vehicles. When changes do occur there will be very intensive KSC/engineering involvement. Examples are provided below describing the traditional Delta and Atlas software verification approaches.

Contractor Software Verification and Test

Boeing Delta/FUSE Mission Example - Mission-peculiar software is routinely subject to intense scrutiny by both Boeing and NASA ELV engineering. Boeing validates flight software in the Systems Integration Laboratory at Huntington Beach which allows full flight simulation capability. NASA is heavily involved in mission design activity and occasionally in the development of flight constants necessary to implement the design. NASA conducts an independent review of the Boeing guidance navigation and control (GNC)/auto-pilot design.

LMA/Atlas Flight Analogous Simulation Test Review (FAST) - This review involves a complete simulation of flight software followed by a two week, in-depth review of all data.

NASA Independent Software Verification and Testing

Boeing/Delta NASA use of software IV&V - In the case of Delta launches NASA typically employs the Aerospace Corporation to conduct independent verification of flight software and mission constants. An excerpt from their Delta/Fuse mission report observed: " No deficiencies were noted in the Boeing verification process. The software code is the same as has been flying on Delta II for some time and no patches or retests have been made for FUSE. It is pointed out that FUSE will be the second flight for a 3-GEM configuration vehicle and Aerospace has not performed an independent evaluation of the control system requirements and have only reviewed the mission constants (sic) set necessary for implementation of given control requirements."

LMA Atlas/GOES Mission Example - KSC/ELV Engineering is responsible for software verification. GRC software verification support is currently in place for the next three Atlas missions, GOES-L, EOS/TERRA, and TDRS-H. For subsequent Atlas launches, software IV&V will be conducted entirely by the KSC-based mission analysis team at KSC. Software IV&V includes the following areas:

Guidance Validation: This review provides a final validation of flight constants. GRC uses a Fortran three degree-of- freedom simulation of Atlas vehicle and a replica of the guidance flight software modules. This activity is considered of extreme importance for planetary missions.

Accuracy Analysis: Monte Carlo-like simulations are conducted for three-sigma variation (root sum of squares combination) in inertial measurement system accuracy. These variations are used to bound potential errors in injection accuracy.

Stability Analysis Validation: Major staging events are simulated as well as passage through maximum dynamic pressure (max-Q).

As noted above, the LMA Flight Analogous Simulation Test Review (FAST) involves a complete simulation of flight software followed by a two week, in-depth review of all data. Typically this review is also supported by five or six GRC-based software experts as well as KSC mission analysis staff. Typical software experts from the controls, guidance, fluids, flight sequencing, and solid motor sequencing areas will participate in the review The FAST review validates all flight software with the exception of the

inertial measurement system.

DCMC Surveillance of Software Development and Test

Boeing/Delta - KSC/SMA/FA delegates software quality assurance functions to DCMC. These functions include, but are not limited to, verifying that all Boeing/NASA quality, configuration management, and test provisions have been followed. Abbreviated excerpts from the proposed Letter of Delegation convey a sense of what surveillance activities DCMC will perform:

"The Agency (DCMC) shall perform Software Quality Assurance per instructions and requirements outlined in the Agency Product and Manufacturing Assurance (P&MA) Plan on a non-interference basis.

The Agency shall perform process control audits on the contractor's design, development, and implementation/release of (CAT A) software, to include new developments of flight software (when required) and unique mission constants. Software reviews may consist of attending critical design reviews (CDR's), configuration reviews, and the like for software items. The Agency shall periodically review contract deliverable (Category A) software documentation, (on a sample basis), for correctness, consistency, and compliance with contract format and content requirements.

LMA/Atlas – The current DCMC surveillance plan (subordinate to the LOD) describes software surveillance activity as follows:

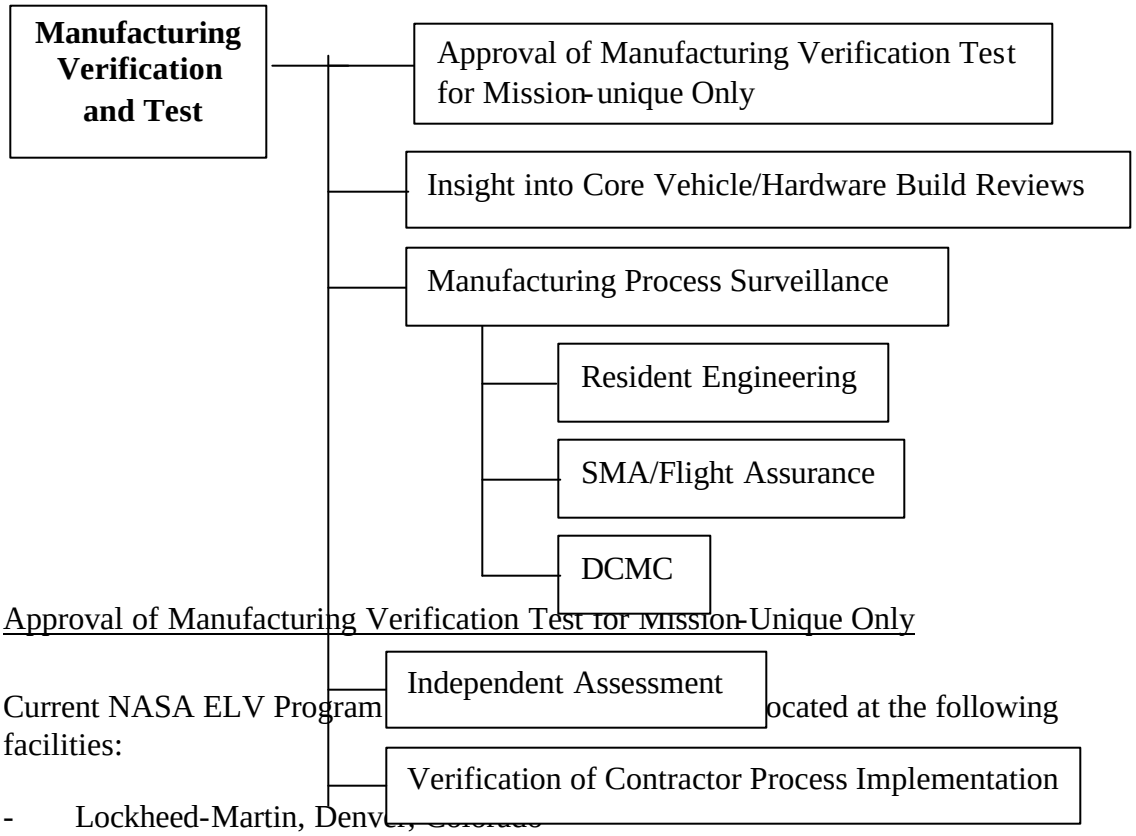
"Software surveillance involves the review and assessment of software development and management on the Atlas program. Included in Atlas software activities are flight software maintenance/updates to support mission requirements. DCMC LMA software quality assurance specialists with support from DCMC engineering personnel, perform the following tasks:

- review software contract deliverables and applicable command media
- attend software build reviews
- review and trend Atlas software trouble reports and software change requests
- monitor FAST and other systems integration laboratory activities
- participate in software audits."

PBMA Section 6.0 - Manufacturing

A.6 Manufacturing Verification and Test Assurance Processes

Manufacturing assurance processes begin with NASA approval authority for NASA mission-unique hardware test and qualification activities. It is worth noting that this represents only a very small percentage of the integrated launch system. Core vehicle assurance comes through the insight process centered on participation in tests, hardware build reviews, and pedigree reviews. In some cases independent assessment performed by the Aerospace Corporation is conducted to certify proper disposition of problems encountered in production (build paper). Another element of insight is manufacturing surveillance carried out by DCMC in support of NASA and other customers. Limited formal verification of contractor assurance process implementation is conducted at the present time. Discussions are underway to find resources necessary to routinely verify implementation of the many assurance processes certified under ISO 9001, and/or listed in contract quality plans, systems effectiveness plans, or equivalent contract assurance requirements.



Approval of Manufacturing Verification Test for Mission-Unique Only

Current NASA ELV Program [illegible] located at the following facilities:

- Lockheed-Martin, Denver, Colorado
- Boeing Corporation, Huntington Beach, California
- Boeing Corporation, Pueblo, Colorado
- Boeing Corporation, El Paso, Texas
- Orbital Corporation, Chandler, Arizona
- Vandenberg Air Force Base, Resident Office

The teams have cognizance of all prime flight critical mechanical and electrical hardware assemblies. Responsibilities include monitoring the current configuration of all prime flight critical mechanical and electrical hardware assemblies, tracking all future Class I modifications and the effects of those modifications on vehicle integration, and the qualification baseline and system reliability. Resident offices are also responsible for evaluating the qualification baseline and acceptance test program for mission-peculiar hardware and first flight items. Resident offices perform hardware pedigree reviews and provide recommendations to NASA concerning all discrepancies involving flight critical assemblies, including any in depth mechanical and electrical analyses necessary to characterize the impact of the discrepancy on mission reliability.

As required, resident engineers perform technical evaluations of the launch vehicle manufacturer's technical reports, quality reports, procedures, and drawings. They also participate in management, engineering, quality, and product reviews in addition to attending meetings on hardware design, manufacturing, testing, inspection, anomaly resolution, and major component pre-ship reviews. Engineering offices place special emphasis on mission-peculiar hardware and flight critical first flight items.

Insight into Core Vehicle/Hardware Build Reviews

LMA/Atlas Example of Supplier Management - The Atlas build reviews are referred to as "Mission Success Reviews." The Denver engineering resident office routinely participates in MSR's at key Atlas/Centaur suppliers. Suppliers that are routinely audited using the MSR process are:

- Honeywell
- Harlingen
- Pratt & Whitney
- Rocketdyne
- Lockheed (Binghamton, New York)
- Marconi
- Thiokol
- Plant 19 (former General Dynamics Tank facility in San Diego

Denver resident office personnel routinely participate in production/manufacturing integrated product teams (e.g., Centaur tank, Atlas tank, and fairing), including LMA and component suppliers.

Boeing/Delta Example of Manufacturing Production Review - Boeing also conducts a series of build reviews which provide an opportunity for NASA engineering and flight assurance personnel to gain valuable insight into core vehicle production issues. Major hardware component build reviews are conducted for the launch vehicle elements/activities listed below. NASA engineering (KSC and residents) as well as flight assurance participate in all Hardware Acceptance Reviews (HAR's) at the Delta prime contractor and major subcontractors.

Typical Delta HAR's are:

- Second Stage Engine
- Main Engine
- Fit-check
- Graphite-Epoxy Motors (GEM's)
- Booster Vehicle Subsystem
- Turnover Review
- Interstage
- Second Stage & Fairing
- Critical Design Review
- Mission Modification Review
- Design Certification Review

LMA/Titan Hardware Production Oversight - While not a requirement under existing MOA's between NASA and the Air Force, the Denver resident engineer office participates in Titan II build reviews. The HAR's give NASA and the Aerospace Corporation the opportunity to review all the build documentation, and nonconformance data on the respective hardware. The HAR's provide valuable insight to the different processes and function of the vehicle and its major components. These reviews are coordinated by the Aerospace Corporation with full participation from NASA. All hardware produced for Titan is reviewed prior to shipment either from the MEC or from LMA in Denver to CCAFS. Flight assurance personnel participated in all the HAR's for the core vehicle and its major element contractors (MEC's).

Manufacturing Process Surveillance

Denver Resident Office Quality Assurance Functions and Tasks - The Denver engineering resident office monitors traditional quality assurance activities including:

- quality assurance issues
- systems engineering issues
- avionics issues

The resident office engineers also participate in Parts Control Board (PCB) and Material Review Board (MRB) meetings as well as in the LMA ISO 9001 Working Group.

SMA/Flight Assurance (LMA Example) - The KSC/FA organization, through its resident assurance engineer (SAIC contractor) in Denver, routinely participates in the production process at Denver. Some of the items covered by the resident assurance representative are engineering review board meetings on Class I design changes, problem report reviews and closure, major nonconformances documented during production, and other miscellaneous activities. The resident assurance engineer also participates via telecon with some of the flight assurance and engineering meetings at KSC. The FAM also monitors the manufacture of the Titan core vehicle, the Centaur upper stage, and the SRMU's. Activities include Class I design changes, nonconformances during manufacture that required an MRB disposition, and general processing concerns at each facility. The FAM also participates in the System Effectiveness Reviews required of LMA by the Air Force. These reviews are held to understand processing problems and initiatives both at LMA and its four MEC's. Further, the FAM conducts monthly reviews

of Corrective Action Problem Summaries (CAPS) initiated by LMA and/or its MEC's. These reviews are held to determine the adequacy of CAPS closures by the contractor. The FAM also attends all of the HAR's conducted on the Titan core, Centaur, and the MEC's. These reviews are held to review the build documentation, nonconformance data, and test results for the major components of the Titan IV vehicle. These are held in parallel with like reviews conducted by Aerospace Corporation.

LMA System Effectiveness Reviews (SER's) - In the past, under GRC management, engineering and flight assurance personnel participated in LMA System Effectiveness Reviews (a review of the product assurance system) conducted in accordance with the in-place Air Force contracts for both Titan and Atlas launch vehicles. These reviews are held on a semi-annual basis and are used to address issues and concerns on the Titan program that affect mission assurance, and to review programs and initiatives being implemented by LMA and/or its MEC's. These reviews provided NASA with valuable insight to the LMA mission assurance activities as well as the opportunity to meet their counterparts at LMA. It is noted that these reviews are evolving toward an ISO-style internal-audit format. It remains to be seen whether or not KSC/ELV/SMA will provide the resources necessary to routinely support these reviews.

Defense Contract Management Command (DCMC) Surveillance - There is not yet, in-place, a coordinated KSC/SMA approach defining DCMC's role within an overall assurance management strategy. Current DCMC letters of delegation (LOD) represent agreements which were in place under GSFC and GRC management of ELV's. KSC/SMA is currently developing a new LOD for the Boeing/Delta program.

DCMC Support for Atlas and Titan - Titan and Atlas production and daily events are monitored by the DCMC. The DCMC has offices at LMA in Denver as well as all the major suppliers. The DCMC role at LMA facilities reflects strong USAF influence in developing requirements and is oriented toward surveillance of a single quality process across multiple government customers. They act only in an oversight role for Atlas vehicles and they do not have hardware approval authority (with the exception of Titan vehicles) at Denver or with the suppliers. In the case of LMA, DCMC is currently working under a GRC LOD. The thrust of the LOD is direction to conduct surveillance. The surveillance plan is the key document delineating specific surveillance activities. The current implementation plan includes audit, manufacturing process surveillance, reliability and maintainability process review, software surveillance, engineering design and development evaluation, observation of the Material Review Board Process (MRB), configuration management surveillance, transportation and shipping process reviews and other administrative support assignments.

DCMC Support for Boeing - The first line of manufacturing assurance is afforded by the ISO 9001 certified processes described in the Boeing PAIP. The contractor has primary responsibility for implementing those processes and assuring that they remain stable, capable, and in control. NASA SMA/FA has insight, albeit limited by available surveillance resources, into prime contractors and major subcontractors through the DCMC personnel resident at manufacturing facilities. The quality assurance functions to be performed on the Boeing/Delta program are set forth in an LOD between NASA and

DCMC. The current LOD provides DCMC support of approximately 7000 hours per year at Huntington Beach and 680 hours per year at the Pueblo manufacturing facility. All DCMC personnel report to the UNISYS Flight Assurance Manager at Huntington Beach, California.

DCMC support typically includes such activities as tracking nonconformances and corrective actions, auditing compliance to the contractor's quality and product assurance plans and processes, conducting parts reviews and inspections, witnessing assembly and test operations, attending contractor-established reviews and monitoring the MRB.

Independent Assessment

Manufacturing activities are subject to periodic independent assessment of hardware fabrication and test. Two examples are provided below:

Boeing/Delta - Aerospace Independent Assessment Example - Each NASA Delta vehicle is subject to an independent contractor (Aerospace Corporation) review of all build paper and test paper deviations, problem reports, non-conformances, or other discrepancies encountered during either fabrication or testing. This review examines disposition of these discrepancies. The Aerospace Corporation refers to this assurance activity as a pedigree review. The pedigree review activity encompasses both hardware and software manufacture/development, and test. The Aerospace Corporation/FUSE review specifically highlighted issues or concerns (all resolved) related to Stage II propulsion, Stage II pneumatics, Stage II regulators, Stage I vernier engines, Stage I solenoid valves, Stage I engine structures, Stage I and II power and control systems, Stage I and II batteries, and vehicle software.

LMA/Titan II Example – Aerospace Independent Assessment Example - The Aerospace Corporation provides independent assessment to the USAF in connection with the manufacturing and test of Titan II and Titan IV hardware and software. The following paragraphs, abstracted from the NASA-managed Titan IIG-7 mission report, characterize the scope and depth of an Aerospace Corporation build review:

> "Aerospace personnel have been involved in the refurbishment and processing of Titan IIG-7, from initiation of core modifications, to processing and acceptance testing of the liquid rocket engines, and acceptance testing of guidance, control and electrical components. Factory testing, as well as launch site acceptance and major system testing, have been reviewed and evaluated for anomalous out-of-family performance. Pedigree packages and qualification testing data on critical components have been reviewed and those components have been found acceptable for flight. Ground systems, facilities, and equipment have been reviewed and their capability to support launch processing have been verified. Aerospace participated with the contractor, LMA, in the Vehicle Readiness Review Team effort to review all processing activity at the launch site, including anomalies and their resolution. All payload integration activities and analyses have been reviewed and the booster to satellite vehicle interface requirements have been identified and verified."

"All systems analyses have been verified, including loads and dynamics, separation, trajectories, and thermal and dynamic environments. Post-flight analysis of previous Titan vehicles and an assessment of the lessons learned were conducted for potential impacts to Titan IIG-7. All Corrective Action Problem Summary (CAPS) impacts were technically evaluated, and have been lifted for this vehicle. The Titan IIG-7 TAG reference trajectory has been validated, and the booster stage II aimpoint and steering data, trajectory performance database, FMH K-factors, propellant margin requirements, ground station telemetry coverage, radio frequency environment, and range safety data have been independently validated, and are acceptable for flight."

"Aerospace is the sole provider of outside verification and validation of Software, Guidance Navigation & Controls (GN&C) and loads for Titan II. The Titan II Flight Program, version XX-U001-7.1-08, was verified by the Aerospace Corporation for the Titan IIG-12 / NOAA-K mission. The binary diskette for the flight code was verified by Aerospace and delivered to the launch site for independent verification of the flight software load on Titan IIG-7. The flight parameters diskettes and the primary and back-up IMU calibration diskettes that are used for independent software load verification for the Titan IIG-7 mission have been verified and validated. All flight parameters are verified to be consistent with the contractor-provided scientific-formatted listing of the flight and IMU parameters. The Titan IIG-7/QuikSCAT booster GN&C/Software mission assurance activities have been completed, certifying that the booster flight software meets mission requirements and supports the mission in the areas investigated."

Verification of Contractor Process Implementation

LMA - NASA "Over the Shoulder Audit" - A past practice of the GRC flight assurance organization, NASA FA managers would participate in LMA internal audits (including major subcontractors) scheduled for the year to verify contractor process implementation and to validate the fidelity of the LMA audit process. Again, it remains to be seen whether or not the SMA/ELV/FA organization will provide resources necessary to resume this surveillance activity.

Boeing - Internal Audit - NASA previously did not participate in Boeing internal audits conducted in preparation for the formal recurrent ISO certification audits. SMA FA now requires DCMC representatives to participate in Boeing internal audits as a means to verify process implementation.

1.2.4 Current ELV Contracts, Prime Contractors, and Principal Manufacturing Sites

Intermediate Expendable Launch Vehicle Services (IELVS) Class

- Atlas (IIA/IIAS/AIII) - Lockheed Martin, Denver, Colorado
- Delta III - Boeing, Huntington Beach, California, and Pueblo, Colorado

Medium Expendable Launch Vehicle Services (MELVS) Class

- Delta II - Boeing, Huntington Beach, California, and Pueblo, Colorado

MED-LITE (ML) Class

- Taurus XL - Orbital Sciences Corporation, Chandler, Arizona, and Dulles, Virginia
- Delta (D3 and D4) - Boeing, Huntington Beach, California, and Pueblo, Colorado

Small Expendable Launch Vehicle Services (SELVS) and Ultra-lite Expendable Launch Vehicle Services (UELVS) Class

- Pegasus - Orbital Sciences Corporation, Chandler, Arizona, and Dulles, Virginia
- Athena I - Lockheed Martin, Denver, Colorado
- LK0 - Coleman Research Corporation, Orlando, Florida

An expanded discussion of the present ELV launch service contracts is provided in Section A.2.

3.2 Probable Causes and Assurance Process Gap Analysis

Failure Case Studies and Gap Analysis

ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjectiv Assessmer High/Medium Probability Mishap Preve
Delta II: 13 Jan 97-Booster Failure Damage or flaw in the Graphite Epoxy Motor case. Undetected during pre-launch testing.	Manufacturing flaws or latent defects difficult to uncover if missed by contractor. In-plant NASA representatives participate in hardware pedigree reviews.	NASA/ELV Mfg. verification processes, i.e., pedigree reviews, build reviews, and test data reviews not likely to have detected a flaw in a motor case.	Low
Titan IV-A20: 12 Aug 98-Booster Cable Short Intermittent shorts on vehicle power bus. Harness insulation was flawed prior to launch and escaped detection during preflight inspections.	Fundamental design issue or poor quality workmanship on just this vehicle.	NASA/ELV Design Verification and/or Mfg. Verification Activities would not likely have detected these failures. DCMC would be most likely to detect the potential failure mode. DCMC supports both NASA and DOD.	Low
Titan IV-B27: 9 Apr 99-IUS Failure (DoD) IUS failed to separate properly. Electrical connector in the separation system failed to disengage. Poorly defined work procedure (involving thermal insulation and tape wrap) identified as root cause.	NASA operational pre-launch/launch review processes are in place. Launch site NASA presence at KSC is an added plus.	NASA/ELV Pre-Flight Verification & Test processes incorporate "Walkdown" activities which may or may not have found the error.	Low/Mediu

ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjectiv Assessmer High/Medium Probability Mishap Preve
Delta III: 4 May 99- RL-10B Failure (DoD) New manufacturing process (engine brazing process) coupled with higher than expected flight loads may have caused the rupture of the combustion chamber.	New (improved) inspection and NDE requirements have been imposed (ultrasound and x-ray) as corrective actions. New manufacturing process changes receive active scrutiny from KSC/ELV program management.	NASA/ELV design verification and/or manufacturing verification assurance activities may or may not have insisted on rigorous manufacturing process qualification and certification for a second tier supplier (P&W).	Low/Mediu
Titan 34D (D-7): 28 Aug 85-1st Stage Engine Shut Down (DoD) Large oxidizer and fuel leaks and turbopump assembly failure.	Three separate and independent failures. Corrective actions were design changes and manufacturing processes.	NASA/ELV design verification and mfg. verifications not likely to have prevented this launch failure.	Low

ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjectiv Assessmer High/Medium Probability Mishap Preve
Titan 34D (D-9): 18 Apr 86-SRM Failure (DoD) Motor case insulation unbonded in one of the vehicle's two SRMs. Hardware quality control need to be tightened.	Poor manufacturing process stability and control.	Current NASA/ELV manufacturing verification (in-factory quality) processes (DCMC) used the same people used by USAF.	Low
Titan 34D (D-3): 02 Sep 88-Transtage Failed To Re-Ignite (DoD) Fuel tank and pressurization lines damaged from repairs or shrapnel impact during pre-launch activities.	One of two causes. Corrective actions included requiring validation and approval of repair procedures. Also cited was improved manufacturing and parts control.	NASA/KSC pre-flight testing assurance processes may or may not have required contractor to show data validating his repair process.	Low
Titan III (CT-2): 14 Mar 90-Intelsat VI Failed To Separate From 2nd Stage Wiring team mis-wired the harness. The satellite never received the separation signal.	Commercial Titan generic composite system test (CST) failed to detect mis-wired configuration.	NASA/KSC pre-flight testing would require use of a spacecraft specific test protocol and would likely have found this error.	Medium

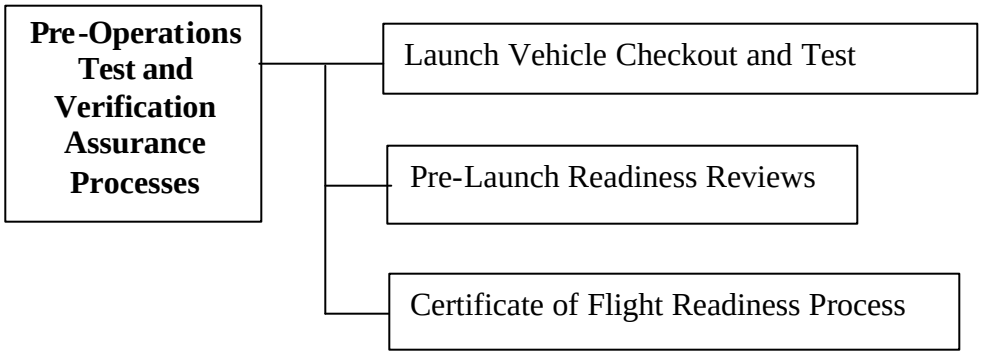
ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessmen High/Medium Probability Mishap Preve
Pegasus XL (Step-3): 22 Jun 95-2nd Stage Nozzle Was Confined And Could Not Gimbal Properly Incorrectly installed skid imparted side force on interstage ring. Ring restricted movement of nozzle. Configuration control practices improved.	Manufacturing assembly errors within Orbital processes.	NASA/ELV manufacturing assurance activities would not likely have been able to detect these errors.	Low

ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assess High/Medium/I Probability of Mi Prevention
Pegasus XL (HETE/SAC-B): 04 Nov 96- Shock Of Stage 2-To-3 Separation Induced Damage To Transient Battery (TB) Corrective action calls for a new TB assembly procedure to include quality assurance verification and new inspection criteria.	This was a first time use of Pegasus dual-satellite capability. Pre-launch the battery was take apart, inspected and reassembled. An unknown failure mode within the battery was identified as the root cause.	NASA GSFC ELV engineering did not detect the failure mode. Even though KSC/ELV engineering focuses on first time use of new designs it is unlikely that KSC would have detected human error in assembly of the battery harness.	Low

PBMA Section 7.0 - Pre-Ops Integ. Test

A.8 Pre-Operations Test and Verification Assurance Processes

Critical NASA assurance activities include the witnessing and verification (insight) of tests and procedures involved in launch vehicle assembly at the launch site and final integration and test on the launch pad. Certain key tests are considered NASA approval items in the early stages of integration. During the final six to nine days on the pad NASA involvement is almost entirely on an approval basis. NASA ELV/engineering, SMA/flight assurance, SMA/quality assurance personnel, and SMA/safety personnel are involved in monitoring on-pad integration activities including final test and check-out of the vehicle. In addition to the test and verification activities, NASA employs a well-documented and proven launch readiness review process culminating in the signing of a CoFR.



Launch Vehicle Checkout and Test

LMA/Atlas Example - The key event in the Atlas pre-flight preparation is the Wet Dress Rehearsal (WDR) in which cryogenic propellants are loaded, tanks are pressurized, and the entire countdown sequence is carried out all the way to launch. The WDR is then followed by a "tiger team" activity lasting a week in which all WDR data are reviewed and all non-conformances are evaluated and corrected. NASA engineering and flight assurance personnel also participate by shadowing LMA personnel performing vehicle walkdown/checklist activities.

LMA/Titan IV Cassini Example: NASA Flight Assurance - NASA GRC Flight Assurance Managers (FAM) attended the ground operations, system integration, and management working group meetings and the integration of Cassini to the vehicle and the pad. They reviewed processing problems encountered during vehicle processing at CCAFS for the first Titan IVB (TIVB-24). This data was used to determine possible processing problems on the Cassini vehicle. They compared Vertical Integration Building (VIB) processing and testing changes made between the TIVB-24 and TIVB-33 core vehicles to confirm all necessary processing and testing was planned and documented. FAM's (as well as KSC-based engineers) participated in the final vehicle readiness reviews of procedures and test data, along with out-of-sequence processing documents. In addition, FA and engineering reviewed all nonconformance and work around documents for possible impacts or oversight of prospective problems.

Typical Launch Service Pre-flight Test and Checkout - The scope of NASA insight and approval in a typical pre-launch test and verification flow is captured in the abstracted sections below derived from the KSC/ELV engineering electrical/mechanical pre-launch test verification and walkdown plan. While not formally documented as a KDP, this plan is typical of the operational level documentation applied to ELV Programs at KSC. All of these activities typically involve ELV/Program discipline engineers and SMA flight assurance and/or quality assurance managers.

- monitor key launch vehicle and payload transportation and handling offload and hardware receiving events
- monitor major system level tests (i.e., propulsion, controls, hydraulics, electrical flight simulation, etc.)
- monitor solid motor build
- observe payload processing events (i.e., fitting attachment , spin balance, etc.)
- observe upper stage motor processing, build-up, balancing, mating, and ordnance installation
- monitor spacecraft processing, weigh/mate operations, installation of clampband, and erection

- monitor all stage erection and mating activity
- monitor spacecraft erection and mate
- monitor mated major systems tests (power-off stray voltage checks, etc.)
- participate in all vehicle walkdown activities

SMA Verification Activities - As part of the pre-launch readiness verification process SMA/FA will typically:

- verify that all high level test data is "in family" (e.g., engine hotfire test data)
- review all special attention items and verify that all fleet issues are resolved pertinent to the relevant hardware
- verify that any open items or incomplete hardware is properly tracked
- verify that all special inspections to this point have been performed satisfactorily
- verify that all waivers and deviations to this point are closed
- provide surveillance of hazardous/high-risk operations

Pre-Launch Readiness Reviews

NMI 8610.24, "Expendable Launch Vehicle (ELV) Launch Services Prelaunch Reviews" establishes the ELV prelaunch review process necessary to assess and certify the readiness for launch of the launch vehicle including separately provided upper stages and supporting launch services provided by commercial companies or by DoD. In accordance with NASA accountability for program mission success, NASA management assesses and certifies the readiness of the launch vehicle (and payload) preparatory to launch through a structured prelaunch review process. Required reviews include:

Center Director's Launch Readiness Review (CD/LRR) - The CD/LRR is held to assess the readiness of the ELV and/or upper stages to proceed with launch site operations. The CD/LRR is chaired by the NASA Center Director of the field installation responsible for management of the NASA Launch Services Projects, or his/her designee, and is held approximately one to two months before launch.

Associate Administrator's Mission Readiness Review (MRR) - The MRR is held to certify the readiness to proceed toward launch countdown. The MRR is chaired by the Associate Administrator for Space Science (AA/SS) and the Associate Administrator of the spacecraft program office (when other than AA/SS), or their designees. The MRR is held at NASA Headquarters after the CD/LRR and approximately one month before launch.

L-4 Review - KSC conducts a Flight Readiness Review (approximately L-4) which is performed prior to the initiation of the final preparations for launch. These reviews include the description of the launch service, mission-unique and first flight items, and anomaly closures from previous missions. At the conclusion of these meetings a poll is conducted to assure that all parties responsible for mission success agree with proceeding to the next milestone.

Launch Readiness Review (LRR) - The LRR is held to update the mission status and closeout actions from the previously held CD/LRR and MRR, and certify the readiness to proceed with initiation of the launch countdown. The LRR is chaired by the NASA Center Directors of the field installations responsible for management of the NASA Launch Services Projects, or his/her designee, and is held approximately two days before launch at the launch site.

Mission Director's Flight Readiness Review (FRR) - The FRR is held to update the mission status, closeout actions from the LRR, authorize approval to proceed into launch countdown, and sign the CoFR. The FRR is chaired by the Mission Director and is held the day before or day of launch at the launch site. Following the FRR and initiation of launch countdown, the final critical milestone before launch is the commit-to-launch poll. The poll, conducted by the NASA Launch Manager for the Mission Director approximately five minutes before launch, asks representatives from all organizational participants to reconfirm their readiness to launch.

NASA may conduct other reviews as appropriate and necessary in preparation for launch. These may include, but are not limited to, Mission Requirements Reviews, Critical Design Reviews, Design Certification Reviews, Preship Reviews, Ground Operations Reviews, and Project and Launch Manager's Reviews. Generally, the mission spacecraft undergoes a parallel prelaunch review process with both the spacecraft and ELV jointly reviewed in the MRR, LRR, and FRR.

Certification of Flight Readiness Process

Following the completion of the Flight Readiness Review, a CoFR is signed by the following parties:

- NASA Spacecraft Mission Director
- NASA Launch Manager (NLM)
- USAF Spacelift Commander
- Launch Service Provider

The NASA SMA organization signs the back-up CoFR that supports the signature of the NASA Launch Manager.

During the launch countdown, the NASA Launch Manager polls the following parties:

- Spacecraft Mission Director
- NASA SMA
- NASA Mission Integration Manager
- NASA Chief Engineer
- NASA Advisory Team

SMA Role in the CoFR Process - Past procedure for obtaining SMA signature on the CoFR has represented an informal collation of information. However, it is anticipated that future SMA CoFR processes will be fully documented and formally incorporate criteria describing the basis for the concurrence (i.e., knowledge and understanding of assurance process implementation.)

3.2 Probable Causes and Assurance Process Gap Analysis

ELV Failure Case Studies and Gap Analysis

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
1.	Delta II: 13 Jan 97-Booster Failure Damage or flaw in the Graphite Epoxy Motor case. Undetected during pre-launch testing.	Manufacturing flaws or latent defects difficult to uncover if missed by contractor. In-plant NASA representatives participate in hardware pedigree reviews.	NASA/ELV Mfg. verification processes, i.e., pedigree reviews, build reviews, and test data reviews not likely to have detected a flaw in a motor case.	Low
2.	**Titan IV-A20: 12 Aug 98-Booster Cable Short** Intermittent shorts on vehicle power bus. Harness insulation was flawed prior to launch and escaped detection during preflight inspections.	Fundamental design issue or poor quality workmanship on just this vehicle.	NASA/ELV Design Verification and/or Mfg. Verification Activities would not likely have detected these failures. DCMC would be most likely to detect the potential failure mode. DCMC supports both NASA and DOD.	Low
3.	**Delta III: 26 Aug 98-Booster Failure** Human error in assumptions regarding applicability of Delta II software on the Delta III vehicle.	Used Delta II software on a Delta III, i.e. wrong application of software. Delta II control software assumed 4 Hz structural vibration modes would be damped (converging toward zero). Classic "heritage trap".	NASA/ELV mission analysis group looks closely at changes to core vehicle software.	Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
4.	**Titan IV-B27: 9 Apr 99-IUS Failure (DoD)** IUS failed to separate properly. Electrical connector in the separation system failed to disengage. Poorly defined work procedure (involving thermal insulation and tape wrap) identified as root cause.	NASA operational pre-launch/launch review processes are in place. Launch site NASA presence at KSC is an added plus.	NASA/ELV Pre-Flight Verification & Test processes incorporate "Walkdown" activities which may or may not have found the error.	Low/Medium
5.	**Athena: 27 Apr 99-Booster Fairing Failure** Shroud failed to separate. Shock unplugged electrical connection. Electrical signal not received.	Greater than anticipated shock associated with initial fairing separation resulted in incomplete final separation. Apparently a design defect - design verification and test failure. Coupled loads analyses should have fully characterized the separation event.	If the vehicle was qualified under NPD 8610.7 then KSC Engineering would not likely have required special fairing/separation qualification testing which might have detected the problem.	Low/Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
6.	**Titan IV-B32: 30 Apr 99- Upper Stage Centaur Software Failure (DoD)** Incorrect flight constant was manually entered into the Centaur software. Human error.	Centaur flight software verification failure. Software experts consulted at GRC do not believe that KSC or GRC would have detected the coding error. One lessons learned, identified by GRC in the failure review, is to have the controls team evaluate the frequency response (Bode Plots) of "implemented software" to verify proper performance.	It is not likely that the NASA/ELV mission analysis group working with LMA would have detected this failure mode. The LMA controls group verified the filter constants (through simulation) but the constant was coded improperly (manual entry) by the software group. The FAST simulation does not exercise the Inertial Measurement System (IMS) software where the error occurred.	Low

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
7.	**Delta III: 4 May 99- RL-10B Failure (DoD)** New manufacturing process (engine brazing process) coupled with higher than expected flight loads may have caused the rupture of the combustion chamber.	New (improved) inspection and NDE requirements have been imposed (ultrasound and x-ray) as corrective actions. New manufacturing process changes receive active scrutiny from KSC/ELV program management.	NASA/ELV design verification and/or manufacturing verification assurance activities may or may not have insisted on rigorous manufacturing process qualification and certification for a second tier supplier (P&W).	Low/Medium
8.	**Atlas-Centaur (AC-62): 09 Jun 84-Upper-Stage Failed To Boost (NASA)** Leak occurred in the LO2 tank. Incorrect clearance between inter-stage adapter and tank. High pressure in tanks at separation.	Failure difficult to mitigate through insight processes.	NASA GRC managed pre-commercial assurance approaches employed at this time. Very unlikely that diminished "insight role" would have detected.	Low

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
11.	**Titan 34D (D-9): 18 Apr 86-SRM Failure (DoD)** Motor case insulation unbonded in one of the vehicle's two SRMs. Hardware quality control need to be tightened.	Poor manufacturing process stability and control.	Current NASA/ELV manufacturing verification (in-factory quality) processes (DCMC) used the same people used by USAF.	Low
13.	**Titan 34D (D-3): 02 Sep 88-Transtage Failed To Re-Ignite (DoD**) Fuel tank and pressurization lines damaged from repairs or shrapnel impact during pre-launch activities.	One of two causes. Corrective actions included requiring validation and approval of repair procedures. Also cited was improved manufacturing and parts control.	NASA/KSC pre-flight testing assurance processes may or may not have required contractor to show data validating his repair process.	Low
14.	**Titan III (CT-2): 14 Mar 90-Intelsat VI Failed To Separate From 2nd Stage** Wiring team mis-wired the harness. The satellite never received the separation signal.	Commercial Titan generic composite system test (CST) failed to detect mis-wired configuration.	NASA/KSC pre-flight testing would require use of a spacecraft specific test protocol and would likely have found this error.	Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
15.	**Atlas-Centaur (AC-70): 18 Apr 91-One Centaur Engine Did Not Achieve Full Thrust** Air ingested into the turbo-pump liquefied and froze in the C-1 engine LH_2 pump and gearbox.	Failure difficult to detect by any secondary insight process. Design and new inspection/procedural corrective actions. New inspections and procedural changes were identified to eliminate debris in the fuel line.	NASA/ELV design engineering processes would have looked closely at a design change. Non-design change failure mode (latent defect) in design would not likely have been detected.	Low
17.	**Atlas-Centaur (AC-71): 22 Aug 92** Centaur C-1 engine failed due to the ingestion of air into the turbo-pump.	Difficult failure scenario to detect. Design and new inspection/procedural corrective actions.	NASA/ELV ERB would have carefully considered return to flight rationale, although a latent design defect would not likely have been detected by NASA/ELV engineering activities.	Low/Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
19.	**Titan IV (K-11): 02 Aug 93-Solid Rocket Motor Exploded** Propellant cut during restrictor repair. The repair was more extensive than had ever been attempted on such a motor segment.	Repairs to safety of flight items are reviewed by NASA representatives. While KSC ELV engineering does not have a solid rocket motor expert they may have sought support from MSFC.	NASA/ELV manufacturing engineering and flight assurance in-plant personnel working with KSC/Engineering may have disallowed use of the segment.	Medium
20.	**Pegasus XL (STEP-1): 27 Jun 94-Inaccurate Estimation Of The Vehicle Aerodynamics**. Erroneous aerodynamic predictions were used to design the flight control autopilot system. Insufficient design verification testing.	Too great a dependence on analysis and modeling coupled with marginal validation of model are root causes.	For first-time vehicle use or newly qualified vehicles there is a greater likelihood that KSC ELV engineering would detect this design defect.	Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
23.	**LMLV-1 (DLV): 15 Aug 95-Thrust Vector Actuation Mechanism Malfunctioned** Erroneous feedback signal caused by reduction of electrical resistance in cables. Cables heated by hydraulic oil ignition. Redesigned hydraulic oil expulsion, improved thermal protection for cables and TVA components.	Three fundamental design failures contributed to vehicle loss. Improper design verification testing is a contributing factor.	NASA/ELV design and engineering processes would not likely have identified these failure modes in a commercial launch mode. If qualifying vehicle for first flight it is possible that NASA would have identified design problems.	Low/medium
24.	**Conestoga 1620: 23 Oct 95-Unintended Thrust Vector Actuation Signal Was Sent To The Castor IVB Nozzle Actuator** No software filters to reduce noise to the onboard navigation computer.	Fundamental design flaws in hydraulics, software, and vehicle modal analysis. Latent design defects. If first flight or qualification flight NASA MSFC (in support of KSC engineering) may have detected design defects.	NASA design/engineering may or may not have identified failure modes in initial vehicle qualification. Post initial qualification NASA would not have been in a mode to capture a latent design defect.	Medium

1.2.6 Current ELV Launch Sites

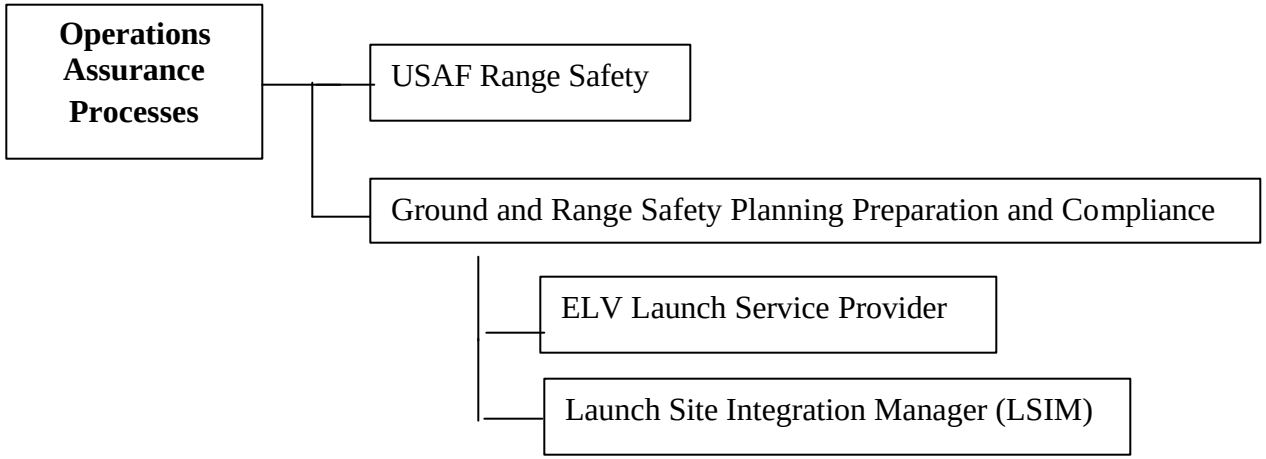
The launch locations which support ELV launches include:

- Eastern Range (Cape Canaveral Air Force Station)
- Western Range (Vandenberg Air Force Base)
- Wallops Island
- Kodiak Island
- Kwajalein Island

A.7 Operations Assurance Processes

Operations assurance processes include all of those activities centered around public safety, worker safety, and payload mission assurance.

In the case of commercially obtained launch services the primary responsibility for safety planning and compliance lies with the launch service provider. The ELV Program Launch Site Integration Manager is responsible for assisting the service provider and the spacecraft customer in fulfilling all safety (and other) launch site requirements. The NASA SMA organization is responsible for assuring the safety of activiities that take place in NASA payload processing facilities. Ultimate range safety responsibilities reside with the Base Commander and are codified in the EWR 127-1 requirements document.



USAF Range Safety

The launch service provider has primary responsibility for interfacing with the USAF 45th Space Wing at KSC and the 30th Space Wing at VAFB to assure compliance with EWR-127-1 requirements for range safety and flight termination system design, manufacturing, and test. NASA/SMA has an insight role in maintaining knowledge and understanding of range safety policy.

Ground and Range Safety Planning Preparation and Compliance

Launch Service Provider Responsibilities for Safety & Assurance - The launch vehicle provider and the USAF have primary responsibility for ground safety activities related to commercial launches from the Cape Canaveral Air Force Station. NASA owns and operates Space Launch Complex (SLC) 2 at VAFB and is responsible for ground safety process implementation at that site.

Generic (All Launch Services) Range And Ground Safety Responsibilities of the Launch Service Provider - Launch service providers are responsible for range support and making provisions for the necessary range approval and scheduling of supporting services for each launch which typically include the following:

- RF radiation clearance

- Fire protection
- Base security, including security police and badge control
- Equipment support
- Shop and laboratory services
- Fluids, gases, and propellants
- Range scheduling
- Range safety functions
- Meteorology
- Communications (local and downrange) data circuits
- Environmental health services
- Metric C-band beacon (radar)
- Telemetry
- Video and still camera coverage of launch
- Station acquisition predictions
- Non-standard servicetracking services (as needed)

Roles And Responsibilities Of Launch Site Integration Manager (LSIM) - The LSIM is the point of contact for customers with payloads to be launched on an expendable launch vehicle and serves as liaison between the customer and KSC management. The LSIM functions in two major arenas: project planning and the ground operation phase at KSC. The LSIM is considered the customer's principal launch site integration interface and as such becomes a source of authority to the payload customer regarding KSC policies, roles and responsibilities, capabilities, and requirements. For major or unique payloads, such as HST, EOS, Cassini, the LSIM may be assigned six to eight years in advance of launch to work long-lead issues.

Other responsibilities include:

- assuring that KSC management and working elements are satisfied with payload plans
- assuring that payload customer is satisfied with KSC planning for their support and operations
- coordinating development of the Launch Site Support Plan

<u>LSIM Safety and Assurance Roles</u>

The LSIM plays a key role in coordinating and assuring compliance with the documentation and planning required by the range under the requirements of
EWR 127-1. The LSIM is responsible for coordinating and verifying the customer development of the Payload Safety Package and the presentation of the document at the Ground Safety Review. The LSIM also verifies the need for special safety waivers and coordinates NASA/SMA surveillance of hazardous operations at least 24 hours in advance.

The LSIM is responsible for assuring that Material Safety Data Sheets (MSDS's) are provided for all hazardous (toxic, biological, and/or radiological) materials. The LSIM is also responsible for confirming that customers have training regarding hazardous material storage, handling, and disposal. The LSIM also plays a safety clearance coordination role with regulatory agencies including, the Department of Energy, the EPA, the State of Florida, and Brevard County, as well as KSC Biomedical and KSC Protection Services.

3.2 Probable Causes and Assurance Process Gap Analysis

ELV Failure Case Studies and Gap Analysis

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
12.	**Atlas-Centaur (AC-67): 26 Mar 87 (NASA)**. Vehicle was struck by lightning. Electrical transient cause erroneous yaw maneuver and loss of vehicle control.	Presently NASA maintains conservative conditions for such a launch. Still, failure occurred under NASA processes.	NASA/KSC and USAF CCAFS have established weather rules and constraints which would prevent a re-occurrence of this mishap.	High